UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/723,119	11/25/2003	Amit Raikar	200300497-1	1279

22879 7590 06/28/2007

HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER	
HOFFMAN, BRANDON S	

ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
06/28/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/723,119	RAIKAR ET AL.	
	Examiner	Art Unit	
	Brandon S. Hoffman	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 November 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *12 April 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-24 are pending in this office action.

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claims 2 and 21 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

4. The term "substantially" in claims 2 and 21 is a relative term which renders the claim indefinite. The term "substantially" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention.

Claim Rejections - 35 USC § 101

5. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

6. Claims 20-22 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claims 20-22 comprise a data structure. Considering a data structure to be "a physical or logical relationship among data elements, designed to support specific data manipulation functions" (IEEE Standard

Dictionary of Electrical and Electronic Terms 308, 5th edition, 1993), this is considered non-functional descriptive material that does not constitute a statutory process, machine, manufacture, or composition of matter.

Claim Rejections - 35 USC § 102

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

8. Claims 1, 3, 4, 20, 23, and 24 are rejected under 35 U.S.C. 102(e) as being anticipated by Resnitzky et al. (U.S. Patent Pub. No. 2004/0068650).

Regarding claims 1, 20, and 23, Resnitzky et al. teaches a method/computer system comprising:

- A first server computer for controlling access to said computer system (fig. 1, ref. num 20);
- A second server computer coupled to said first server computer for providing control of said computer system (fig. 1, ref. num 90);
- Computer usable media comprising computer usable instructions that when executed on a processor of said first server computer implement a method of

establishing a consistent password policy, said method comprising (paragraph 0111):

- Accessing a computer usable password policy data structure by a password policy enforcement agent (paragraph 0107-0110); and
- Enforcing a password policy described within said password policy data structure by said password policy enforcement agent (paragraph 0111).

Regarding claim 3, Resnitzky et al. teaches wherein said password policy enforcement agent is operable on a client computer of a client-server computer system (fig. 2).

Regarding claims 4 and 24, Resnitzky et al. teaches operable on a utility data center (fig. 4).

Regarding claim 5, Resnitzky et al. teaches further comprising validating said computer usable password policy data structure for authenticity by said password policy enforcement agent (paragraph 0108).

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claims 2, 19, and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Resnitzky et al. (U.S. Patent Pub. No. 2004/0068650) in view of Cole et al. (U.S. Patent Pub. No. 2002/0161707).

Regarding claims 2 and 21, Resnitzky et al. teaches all the limitations of claims 1 and 20, respectively, above. However, Resnitzky et al. does not teach wherein said computer usable password policy data structure comprises a file structure substantially compatible with extensible markup language.

Cole et al. teaches wherein said computer usable password policy data structure comprises a file structure substantially compatible with extensible markup language (paragraph 0095).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine using XML for the data structure, as taught by Cole et al., with the method of Resnitzky et al. It would have been obvious for such modifications because XML's primary purpose is to facilitate the sharing of data across different information systems.

Regarding claim 19, Resnitzky et al. teaches all the limitations of claim 1, above. However, Resnitzky et al. does not teach further comprising providing, by said

password policy enforcement agent, feedback to a configuration and aggregation point, about which of said plurality of password policies have been successfully enforced.

Cole et al. teaches further comprising providing, by said password policy enforcement agent, feedback to a configuration and aggregation point, about which of said plurality of password policies have been successfully enforced (paragraph 0083).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine providing feedback for successful enforcement, as taught by Cole et al., with the method of Resnitzky et al. It would have been obvious for such modifications because feedback informs the user/administrator that the policy being enforced is working.

Claims 5-18 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Resnitzky et al. (U.S. Patent Pub. No. 2004/0068650) in view of Password Policy of eRA (referred to as Password Policy hereinafter).

Regarding claims 5-18 and 22, Resnitzky et al. teaches all the limitations of claims 1 and 20, above. However, Resnitzky et al. does not teach specific policy types.

Password Policy teaches comprising a computer access password policy parameter selected from the set of computer access password policy parameters

comprising: a threshold parameter for unsuccessful access attempts that when exceeded disables a computer system access account; a parameter indicating the a time duration within which said threshold parameter number of unsuccessful access attempts triggers locking of a computer system access account; an initial delay parameter to block access to a computer system access account for a period of time after an unsuccessful access attempt; a minimum password length parameter; a maximum password length parameter; a parameter to prohibit passwords consisting of a natural language word; a parameter to prohibit passwords consisting of a palindrome; a parameter to prohibit passwords consisting of a derivative of a computer system account name; a parameter to automatically generate a password; a parameter to automatically generate a pronounceable password consistent with all of said plurality of password policies; and a parameter to specify a set of characters utilizable to automatically generate a password (page 2-4, section 5.0 through 5.5).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine a plurality of different password policies, as taught by Password Policy, with the method/computer system of Resnitzky et al. It would have been obvious for such modifications because the policies taught by Password Policy reduce the risk of unauthorized access to servers and databases (see page 1, section 1.0 of Password Policy).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon S. Hoffman whose telephone number is 571-272-3863. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Brandon Hoffman/

BH

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

6/23/07

PASSWORD POLICY FOR eRA
July 17, 2003

1.0 Purpose

This policy is intended to reduce the risk of unauthorized access to servers and databases essential to the mission of eRA. It defines:

- strong password standards
- password lifetimes
- guidance for password policy verification
- guidance for the establishment of passwords and modification of passwords
- Compliance and enforcement procedures

This policy addresses the risk of weak passwords as well as password disclosure – intentional or unintentional, malicious or benign – and hence, unauthorized access to servers and data.

2.0 Background

It is a well-established principle of IT security that strong passwords are an important part of any organization's security posture. Weak passwords can lead to unauthorized access. Such access would threaten the information whose integrity is essential to the mission of eRA and the National Institutes of Health. Easily guessable passwords are one of the most common ways to accomplish unauthorized access to any system. The National Institute of Standards and Technology suggests several ways to assist in the mitigation of the risks associated with unauthorized access by using better password policies in their document Generally Accepted Principles and Practices for Securing Information Technology Systems, URL; http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf. NIST suggests that organizations clearly specify required password attributes. These should include minimum and maximum lengths, the type of characters that are acceptable, and contextual criteria. NIST goes on to suggest that passwords should be changed periodically and that users should be trained in good password selection.

3.0 Related Documents

NIH Password Policy, http://irm.cit.nih.gov/policy/passwords.html
NIH Guidance for Good Passwords,
http://irm.cit.nih.gov/policy/passwords.html

DHHS Automated Information Systems Security Program Handbook, http://irm.cit.nih.gov/policy/passwords.html
DHHS Personnel Security Suitability Program, http://www.hhs.gov/ohr/manual/98_1.doc

4.0 Scope

This policy applies to all users who access eRA servers and databases, including development and test servers and databases, as well as the personal workstations used to access these servers and databases.

5.0 Policy
Unless specifically stated otherwise, the items in this section apply to both end user and system level accounts and passwords.

5.1 Requirements

- Each user must have a unique username.
- Each IC through a Memorandum of Understanding (MOU) will accomplish suitability determination for each end user.
- Initial passwords must be communicated to the user securely.
- Unless created by the user, initial passwords are pre-expired.
- Passwords for system level accounts, application administrative accounts, system administrator accounts, and database administrator accounts:
    - Must be changed at least every 90 days.
    - Initial password must be changed by logging into the system within 5 days of issue.
- End user passwords must be changed at least every 180 days.
- Accounts associated with passwords that have been expired for more than 45 days will be deleted unless there is a business reason to retain the account, e.g. principal investigator that logs on once or twice a year.
- Authentication must be to individual users, not groups.
- No passwords are to be stored in clear text.
- No password will be given to a user, an account unlocked, or a password changed without the identity of the user being properly validated by the Account Administrator.

5.2 Password Guidance

- The password cannot contain the user's own or close friend's or relative's name, employee number, social security number, birthday, significant anniversary, telephone number, address, or any other information about the user that could be easily guessed or discovered.
- Passwords must not contain common words or words found in any dictionary.
- Keyboard patterns cannot be used, e.g. qwerty.
- Passwords must be changed immediately if they have been given to someone else.
- To prevent accidental disclosure the following precautions must be taken:

    - Passwords must not be disclosed to anyone, including anyone claiming to be User Support Branch Staff or high ranking eRA management.
    - Passwords must be stored in an encrypted form on any file, including a PDA.
    - Users should not communicate his/her password or password paraphrase in an email.
    - Passwords should not be written down.
    - New passwords cannot be a simple change of the previous password, e.g. adding a number at the beginning or end, changing one letter or number.
- The Principle of Least Privilege must be used in assigning privileges to accounts.
- Unique passwords must be used on each server.

5.3 Password Formulation Standards

- Password length must be 8 or greater characters.
- Must contain a mixture of alpha and numeric characters, as well as special characters.
- The first and last characters must not contain numbers.
- The password cannot contain the user's login name.

5.4 Password Change Requirements

- Passwords cannot be reused for a period of one year.
- Passwords must be changed as soon as possible after a compromise and within one business day.

- A password must be changed if directed to do so by User Support Branch Personnel.

5.5 Protecting Passwords

- The account will be locked after 5 consecutive unsuccessful login attempts as specified in the procedures associated with this policy.

6.0 Responsibility

The User Support Branch (USB) acts as the point of contact for the NIH Office of the Director (OD) and the Division of Extramural Information Systems (DEIS) for all users requiring new accounts, roles, password changes, and the reporting of possible compromises as well as any other issues involving user accounts. For all other ICs and OPDIVS this authority is delegated to the eRA/IMPAC II Coordinators within that IC/OPDIV who can in turn delegate the actually management of accounts and access to the User Admin Module to IC/OPDIV staff as appropriate. Requests for IC/OPDIV staff access to the User Admin Module must be made by the eRA/IMPAC II Coordinator in writing (email acceptable) to USB. IC/OPDIV accounts will be reviewed and validated by the USB at least annually. The USB also acts as a liaison between the user and the System Operations Management Branch (SOMB). The USB works with IC and Institution staff to ensure that accounts are closed on all relevant servers and applications where a user account is no longer needed.

The Systems Operations Management Branch (SOMB) sets up user accounts according to this policy when contacted by USB. No new account is established until the user has signed a user policy form that has been validated by the Accounts Administrator.

The Information System Security Officer (ISSO) is responsible for ensuring that this policy is followed. She/he is also responsible for all changes to this policy. The ISSO is responsible for auditing the compliance with the policy. The ISSO makes recommendations for modifications that it deems necessary to the eRA management.

Users are responsible for protecting their passwords and reporting any compromise promptly to the USB. They are also responsible for selecting strong passwords.

Management is responsible for ensuring that users are aware of this policy. They also must be consistent in the enforcement of this policy.

7.0 Compliance

All servers have the Operating System configured to enforce this policy. The USB does periodic "social engineering" checks to ensure that users do not divulge passwords. Users who repeatedly choose weak passwords are subject to either restricted access or possible disciplinary action if they choose weak passwords for four consecutive months.

8.0 Enforcement

If identified password policy violations are not corrected within one business day, the account is locked. If repeated violations occur, the employee is subject to termination. Management ensures the uniform enforcement of this policy.

9.0 Revision history

This is a new policy. There is no existing policy that is made obsolete by this policy.

/s/James Cain
Director, DEIS

_____
Date